El Mando Conjunto de Ciberdefensa y la seguridad nacional

El ciberespacio ofrece numerosas oportunidades pero su misma arquitectura lleva asociado un número no menor de riesgos y vulnerabilidades. El Mando Conjunto de Ciberdefensa (MCCD) nació hace algo más de dos años con la misión de proteger las redes del Ministerio de Defensa y aquellas que, por su carácter estratégico, puedan asignársele, de estas amenazas. En el Mando, militares de los tres ejércitos trabajan día a día para fortalecer sus capacidades en el siempre cambiante escenario cibernético.

TENIENTE CORONEL ÁNGEL GÓMEZ DE ÁGREDA
Mando Conjunto de Ciberdefensa

El hecho de que el ciberespacio sea un ámbito artificial basado en los avances tecnológicos en los campos de la informática y las comunicaciones parece distorsionar, en ocasiones, su verdadera naturaleza como hábitat humano. Por mucho que la arquitectura de las redes, su diseño y evolución tenga que ir de la mano de los avances que se produzcan en aquellos campos, el uso de las mismas y sus efectos hace tiempo que han pasado a ser del dominio de lo social. El ciberespacio se ha convertido en la biosfera digital en la que nuestros avatares nos representan en una existencia tan real como la de la biosfera física.

Este matiz es de gran trascendencia porque, si bien las ecuaciones y algoritmos que rigen el funcionamiento de la capa técnica del ciberespacio son predecibles y programables, la actividad humana que se desarrolla tomando como base el entorno digital sigue sometida a las mismas contradicciones y vicisitudes de las personas de carne y hueso que la ejecutan. Las mismas fortalezas y debilidades de la condición humana se reflejan en el mundo ciber magnificadas por el factor multiplicador que aportan las características de internet.

Es por ello que conviene recordar siempre que la tecnología no es más que el soporte del ciberespacio. Las redes son un medio y no un fin en sí mismo, y los retos y oportunidades que se presentan a través de ellas siguen teniendo la misma dimensión humana de siempre. El ciberespacio es el hábitat natural del conocimiento, no de la tecnología exclusivamente. Por él se mueven nuestros datos, que nos cosifican y nos transforman en un registro más de una base de datos, y nuestras ideas, que nos definen y nos permiten desarrollarnos

como individuos. Una aparente contradicción que muestra el enorme potencial de internet para cambiar la sociedad en la que vivimos.

Una sociedad digital

Las redes se basan en nodos físicos concretos, pero su fortaleza viene dada por los vínculos que se establecen entre ellos. La verdadera dimensión de cualquier actor en el ciberespacio se mide, no por sus capacidades, sino por las interacciones que es capaz de desarrollar. Este concepto se ilustra muy bien en las redes sociales y sus legiones de "amigos" y "seguidores" que tanto condiciona el comportamiento de sus miembros. El valor de cada uno viene dado por su porfolio de contactos. En este sentido, internet es un factor igualador y democratizador con el potencial de alterar nuestras relaciones fuera de la red.

Por otro lado, el alcance global, ubicuo y anonimizado de las acciones que se desarrollan en la red supone un riesgo para esa misma individualidad. La labor uniformadora y conformadora de opiniones que ya tuvieron la prensa escrita, la radio o la televisión da un salto cualitativo con la interactividad que añade el uso de internet. En la red, las ideas se construyen —real o aparentemente— de forma cooperativa y se incorporan al acerbo individual como consensos en los que se ha participado. De este modo, la idea se interioriza mucho más que la que se recibe de forma pasiva y no dialéctica.

Estas características del ciberespacio convierten a la biosfera digital en un ámbito de confrontación más para el ser humano, si bien con características peculiares. En las redes el conflicto es permanente y siempre tiene múltiples frentes abiertos; un escenario de cooperación-competición que aprovecha las pasarelas entre el mundo físico y el lógico para actuar en ambos.

De la guerra

En la guerra, como en otras muchas actividades humanas, el objetivo final es la preponderancia de las ideas o intereses propios sobre los ajenos. No se trata tanto de destruir al enemigo como de doblegarlo a nuestra voluntad **(1)** . La aceptación de nuestros postulados puede venir impuesta por la coerción física o por la convicción lógica, aparentemente menos intrusiva. El ciberespacio nos ofrece una herramienta ideal para llevar a cabo ambos tipos de acciones como demuestran los innumerables ejemplos que ya tenemos después de unos pocos años.

En el ciberespacio, por lo tanto, el conflicto es una actividad permanente —si bien, normalmente, de bajo nivel— que se desarrolla en múltiples frentes dentro y fuera de la estructura propia de los ministerios de defensa correspondientes. Las acciones bélicas digitales llevan ya un tiempo estando presentes en todos los conflictos armados convencionales, pero también se desarrollan independientemente fuera de los mismos.

Se han llevado a cabo ataques informáticos independientes a nivel estatal como los de Estonia o Kirguistán, se han acompañado acciones bélicas convencionales con agresiones cibernéticas en ocasiones como Georgia o Ucrania, se han atacado infraestructuras estratégicas como la central de Natanz (Irán) o el gasoducto BTC (Turquía), se han obtenido datos tecnológicos que reconfiguran el equilibrio geoestratégico de grandes regiones del mundo como en la intrusión en Lockheed Martin a través de RSA con el robo de información sobre el avión JSF **(2)** .

Estas acciones, ya clásicas del conflicto cibernético, ilustran la diversidad de aspectos que tienen que protegerse para salvaguardar la Seguridad Nacional, el bienestar de la población y la libertad de acción en el ciberespacio en beneficio propio. Tan amplias como puedan parecer, no son más que una pequeña parte de las modalidades de ataque que ya han tenido lugar. La juventud y amplitud de este ámbito propician que sigan apareciendo nuevas formas de acción cada vez con mayor frecuencia. Cada una de ellas, las que ya conocemos y las que estamos sufriendo o sufriremos próximamente tienen a su vez, multitud de derivadas.

Un ataque, como el de la guerra de Georgia, asociado a una acción bélica cinética puede dirigirse a la denegación de los servicios esenciales de la nación, o a los de mando y control de las operaciones militares, o a las comunicaciones, o tener como objetivo la obtención de inteligencia sobre el enemigo, o la alteración de la información en poder del adversario para inducirle a tomar decisiones equivocadas o inapropiadas. Todos ellos con la misma herramienta. En agosto de 2008, los principales efectos de las agresiones cibernéticas que sufrió Georgia se produjeron sobre la moral de una población que se vio privada de sus comunicaciones con el exterior y de visibilidad sobre la reacción internacional al conflicto que sufría.

Un mundo sin fin

Las Fuerzas Armadas de los países ya no pueden limitar su vigilancia a las acciones potencialmente hostiles de otros ejércitos y actores nacionales. El número de potenciales agresores ha dejado de verse limitado por el alcance físico de los mismos, o por su potencia de fuego. Hoy son 3.000 millones de internautas los que deambulan por la red; aliados o adversarios según el momento y las circunstancias, pero siempre actores activos.

Las grandes corporaciones, los grupos de presión y de interés, la delincuencia organizada y, desde luego, las organizaciones y grupos terroristas han encontrado en la red un terreno abonado para ejercer su influencia con mayor alcance e impunidad que nunca. De entre ellos, los grupos yihadistas se muestran cada día más activos en la utilización de internet y su potencial. Desde las burdas páginas elaboradas por los talibán afganos de hace unos años hasta Dabiq **(3)**, la revista digital editada por el autodenominado Estado Islámico y elaborada con altos estándares de calidad, hay un salto evolutivo muy significativo.

La misma estructura de la red propicia una cierta "externalización" de la actividad criminal y ciber-bélica. La subcontratación de los ataques en grupos de hackers expertos o de universidades y empresas especializadas es una tendencia que complica, aún más, la identificación del atacante y la atribución de la autoría de las agresiones.

El Mando Conjunto de Ciberdefensa

España, como otros países avanzados, se ha dotado de una Estrategia de Ciberseguridad Nacional **(4)** que define sus objetivos en la materia y apunta la forma de alcanzarlos. De forma casi simultánea nació el Mando Conjunto de Ciberdefensa (MCCD) **(5)** con la misión de asegurar las redes del Ministerio de Defensa y aquellas que se le pudieran asignar. El colofón de este proceso iterativo es la elaboración de un Plan Nacional de Ciberseguridad y la finalización de la definición de las estructuras que permitan que los organismos que las forman actúen con la mayor eficacia y eficiencia.

Para cumplir su misión, el Mando Conjunto de Ciberdefensa necesita dotarse de las tres capacidades básicas que ha definido: la de defensa de sus propias redes y sistemas, de la explotación de las oportunidades que ofrece este medio, así como la de respuesta a las agresiones a fin de contribuir al esfuerzo conjunto de España para establecer un entorno seguro en

Ciberseguridad y ciberdefensa forman parte de un mismo abanico de herramientas y procedimientos del que las naciones tienen que disponer para garantizar su libertad

la red, tanto a nivel nacional como internacional.

El MCCD se ha dotado de una estructura clásica pero flexible, que intenta adaptarse tanto al resto de los organismos del Ministerio de Defensa como a la idiosincrasia cooperativa del ciberespacio. En su Jefatura de Operaciones se ha ubicado el CERT que actúa como instrumento técnico de defensa y coordinación. El embrión, que alcanzó la Capacidad Operativa Inicial en septiembre de 2013, continúa creciendo sobre una base sólida en un entorno tan cambiante como el de las misiones militares del siglo XXI.

Ciberseguridad y ciberdefensa forman parte, pues, de un mismo abanico de herramientas y procedimientos del que las naciones tienen que disponer para garantizar su libertad. El gran potencial del ciberespacio para llevar a cabo agresiones y los muy diferentes grados de concienciación, entre unos y otros actores, magnifican la importancia de la componente ciber durante este periodo de transición hasta que lo digital haya sido incorporado plenamente a nuestra doctrina y a nuestros modos de operación habituales en toda su extensión. El ciberespacio ya ha dejado de ser un mero medio auxiliar que facilita las transmisiones y su operacionalización, como ha expresado el Almirante Rogers, jefe del US CyberCommand, es una prioridad para todos. .

NOTAS

(1) Carl Von Clausewitz en "De la guerra": "La guerra es un acto de violencia que intenta obligar al enemigo a someterse a nuestra voluntad."

(2) Una descripción más detallada aparece en el capítulo IV de "El Ciberespacio, nuevo escenario de confrontación", monografía 126 del CESEDEN, editada por el Ministerio de Defensa en febrero de 2012 y disponible en *http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf*

(3) *http://media.clarionproject.org/files/islamic-state/islamic-state-isis-magazine-Issue-4-the-failed-crusade.pdf.*

(4) *http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf* .

(5) *http://www.emad.mde.es/CIBERDEFENSA/*